REMARKS/ARGUMENTS

35 U.S.C. §102 Rejections

In the Office Action, Claims 1-4, 6, 8, 9, 11-24, 26-31, 34-39, 41, 42, 44-52, 54, 56, 57, 59-61 were rejected as being anticipated by Published U.S. Patent application No. 2003/0046238 to Nonaka et al. (hereinafter "Nonaka"). Applicant respectfully submits that these claims, as amended, are patentable over Nonaka.

Independent Claims 1, 31, 34, and 49 have been amended to clarify that "the present invention can store rights and/or usage information *in clear form* on a client device while still providing security for the content and integrity for the rights/usage information." *See* the published version of the current application (No. 2005/0022025) (hereinafter "Current Application") at paragraph [0017] (emphasis added); *see also* Current Application Figure 3A (340, store rights and/or usage information in clear form). Independent Claim 20, as originally written, claims "storing the rights information… at the client device in a *clear form*." (emphasis added) Storing the information in clear form is beneficial because it can greatly simplify rights enforcement and/or usage reporting because the information does not need to be decrypted before it can be read or used either on the client device or by an external device. This simplification is especially advantageous when a simple, inexpensive client device lacks resources to do unnecessary decryption. By contrast, Nonaka does not teach that rights and/or usage information may be stored in clear form. Thus, Nonaka does not teach or suggest any of the advantages that may be gained by storing rights information in a clear form.

Because Nonaka teaches that rights information must be stored in encrypted form, and because what is claimed stores rights information in clear form, Applicant respectfully submits that the Examiner has not established a *prima facie* case for anticipation. To establish a prima facie case of anticipation, the Examiner is obligated to identify where "each and every facet of the claimed invention is disclosed in the applied reference." *Ex parte Levy,* 17 U.S.P.2d 1461, 1462 (Bd. Pat. App. & Intef. 1990). Furthermore, anticipation requires that each and every claim element must be identical to a corresponding element in the applied reference. *Glaverbel Société Anonyme v. Northlake Mktg. & Supply, Inc.,* 45 F.3d 1550, 1554 (Fed. Cir. 1995). The Office Action fails to present such a *prima facie* case of anticipation.

Claims 1, 31, 34, 49

As stated many times in the Office Action, Nonaka teaches that Usage Control Policy (UCP, i.e. rights) information is used to create an *encrypted* content key, which is then used to encrypt content data. Nonaka paragraph [0019], lines 1-6; *see also, e.g.,* Nonaka paragraph [0250] (UCP data transmitted in a secure container). In other words, Nonaka teaches that the UCP (rights) information is the encryption key that is required to decrypt the content data; it would therefore make little sense to store the UCP information (the "key" to the content) in clear form. Rather, Nonaka makes it clear that the rights information is stored in a secure, encrypted fashion. *See, e.g.,* Nonaka paragraphs [0019], [0246], [0250], Figure 3B (illustrating an encrypted container, *see* paragraph [0069], enclosing UCP data), Figure 5 (illustrating UCP data stored in ciphertext), Figure 9 (illustrating UCP data stored in an encrypted container).

By contrast, amended Claim 1 reads as follows:

1. A method comprising:

obtaining an integrity hash of rights information stored **in a clear form** at a client device, said rights information being associated with content stored at the client device;

encrypting the integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device; and

storing the encrypted hash on the client device.

(emphasis added) Storing the information in clear form provides a level of functionality and convenience that is not taught or suggested by Nonaka, a level of functionality that is in fact antithetical to the teaching of Nonaka. Specifically,

> [s]toring the information in clear form can greatly simplify rights enforcement and/or usage reporting because the information does not need to be decrypted before it can be read or used either on the client device or by an external device. Security and integrity can be provided on the client device by using a device key that is externally inaccessible from the client device, reducing or eliminating the need to depend on externally known secrets. For example, a client device, such as an MP3 player or PDA, often includes a hardware key embedded within the device.

Current Application, paragraph [0017]. Furthermore, this simplification is especially advantageous when a simple, inexpensive client device lacks resources to do unnecessary decryption. *See* Current Application, paragraph [0006]. Accordingly, Nonaka does not anticipate Claims 1, 31, 34, and 49.

Claims 2-4, 6, 8-9, 11-19, 35-39, 41, 42, 44-48, 50-52, 54, 56, 57, 59-61

As an initial matter, Claims 2-4, 6, 8-9, 11-19, 35-39, 41, 42, 44-48, 50-52, 54, 56, 57, 59-61 depend from allowable independent claims and are therefore allowable for the reasons noted above. However, there are additional bases on which to allow these claims.

For example, Nonaka does not anticipate Claims 4, 37, and 52 because Nonaka does not teach the use of a client device key. In asserting that Nonaka anticipates Claims 4, 37, and 52, the Examiner analogizes Nonaka's "license key" to the current application's "client device key." However, the Applicant respectfully submits that this analogy is flawed because Nonaka's license key serves a very different function than the current application's client device key. The current application describes the client device key as follows, "Security and integrity can be provided on the client device by using a device key that is externally inaccessible from the client device.... For example, a client device...often includes a hardware key embedded within the device. The hardware key ... is usually not accessible through any external data paths...." Current application paragraph [0017]. Thus, a client device key typically has at least two salient characteristics: it is accessible only inside the client device, and it is implicitly a unique, static key associated with one specific client device.

Nonaka's license key differs from the client device key in several respects. First, Nonaka teaches that a license key may be sent across a network to a client device. *See* Nonaka, paragraph [0099], [0304]. Thus, a license key must be accessible through an external data path. Second, a license key is associated with a particular piece of content and may define a period of time for which that piece of content is licensed. *See* Nonaka, paragraph [0036], [0305], [0306]. Also, a license key may change, as Nonaka teaches that a license key must be periodically updated. *See* Nonaka, paragraph [0305], [0306]. Thus, a license key is not unique to a client device, nor is it static. Accordingly, because a license key cannot be analogized to a client device key, the Applicant respectfully submits that Nonaka does not anticipate Claims 4, 37, and 52.

For another example, Nonaka does not anticipate Claims 11, 12, 44, and 60 because, as discussed at length above, Nonaka does not teach storing or transferring rights information in clear form.

For a third example, Nonaka does not anticipate Claims 13, 28-30, 45, and 61 because Nonaka does not, so far as Applicant can discern, teach tracking usage of the content. The Examiner relies on Nonaka paragraph [0053] to support the assertion that Nonaka anticipates Claims 13, 28-30, 45, and 61. However, that paragraph discusses "a data processing system" that,

among other things, appears only to determine price and usage restrictions for purchased content. Applicant is unable to locate any information in that paragraph or elsewhere in Nonaka that teaches tracking the usage of content. Thus, Nonaka does not anticipate Claims 13, 28-30, 45, and 61.

For a fourth example, Applicant cannot discern what language in Nonaka paragraphs [0339], [0346], or anywhere else in Nonaka teaches granting unlimited play for the content on the client device. The referenced paragraphs disclose that a playback module exists and that the playback module can, unsurprisingly, play back content data. However, Claim 18 (and amended Claim 59) specify that the rights information grants *unlimited* play, unlimited play that is nowhere taught by Nonaka. Accordingly, Nonaka does not anticipate Claim 18.

There are other examples of additional reasons why Nonaka does not anticipate Claims 2-4, 6, 8-9, 11-19, 35-39, 41, 42, 44-48, 50-52, 54, 56, 57, 59-61, but for the sake of expediency and because all of those Claims depend from allowable independent claims and are therefore allowable, Applicant need not further discuss these additional reasons.

Claim 20

Claim 20, as originally written, includes "storing the rights information and the first integrity hash at the client device in a clear form." As discussed generally above, Nonaka does not teach or suggest storing rights information in clear form. Therefore, the references cited by the Examiner do not anticipate this step of Claim 20. Specifically, Nonaka paragraph [0246], lines 1-4 teaches an *encrypted* ("secure") storage container for content key data. *See also* Nonaka Figure 10 (information in secure container stored in cyphertext). Similarly, Nonaka paragraph [0019] teaches storing rights information in an encrypted form. Nonaka paragraph [0339] teaches only that a client device exists, not that the client device stores rights information in a clear form. On the contrary, as discussed above, Nonaka teaches that rights information is used as the basis of the key for encrypting the content data; therefore, to ensure the security of the content data, Nonaka teaches that rights information must not be stored in clear form. Accordingly, Nonaka does not anticipate Claim 20.

Claims 21-24, 26-30

Claims 21-24, 26-30 depend from allowable independent Claim 20 and are therefore allowable for the reasons noted above. Similar to Claims 2-4, 6, 8-9, 11-19, 35-39, 41, 42, 44-48, 50-52, 54, 56, 57, 59-61, there are numerous additional reasons that Claims 21-24, 26-30 are

allowable. As just one example, Claim 26 is allowable because, as discussed at length above, Nonaka does not teach storing or transferring rights information in clear form. As with Claims 2-4, 6, 8-9, 11-19, 35-39, 41, 42, 44-48, 50-52, 54, 56, 57, 59-61, there are other examples of why Nonaka does not anticipate Claims 21-24, 26-30; however, Applicant need not go further into those reasons because Claims 21-24, 26-30 are allowable because they depend from allowable independent Claim 20.

35 U.S.C. §103 Rejections

Claims 5, 7, 25, 40, 53, 55

In the Office Action, Claims 5, 7, 25, 40, 53, 55 were rejected as being obvious considering Nonaka in view of Serret-Avila's US Patent No. 6,959,384 (hereinafter "Serret-Avila"). Applicant respectfully submits that these claims are patentable over Nonaka in view of Serret-Avila.

As an initial matter, Claims 5, 7, 25, 40, 53, 55 all depend from independent Claims that are allowable because, as discussed above, Nonaka does not teach or suggest storing rights information in clear form. Therefore, Claims 5, 7, 25, 40, 53, 55 are allowable because they depend from allowable independent claims. However, Claims 5, 7, 25, 40, 53, 55 are also allowable for additional reasons. The following is a nonexclusive listing of additional reasons why Claims 5, 7, 25, 40, 53, 55 are allowable.

Claims 5, 7, 25, 40, 53, 55 are allowable because one of ordinary skill in the art to which the subject matter sought to be patented pertains would not have been motivated to modify Nonaka as taught by Serret-Avila. The subject matter sought to be patented pertains to rights enforcement and usage reporting. Current Application paragraph [0001]. More specifically, it pertains to storing rights information and providing security for content data stored on a client device, a client device that may or may not have the resources to manage content and external communications. *See* Current Application paragraph [0006], [0017].

A person of ordinary skill in that art would not have been motivated to consider the teachings of Serret-Avila because Serret-Avila pertains to subject matter that is at most only distantly related to the problems of storing rights and usage information on a client device. Specifically, Serret-Avila pertains to the authentication of very large, streaming media files. *See, e.g.,* Serret-Avila, column 2, lines 31-49; column 3, lines 2, 9, 19, 60. While both Serret-Avila

and the present invention broadly relate to electronic data, the similarities stop there. A person of ordinary skill working with the subject matter of the present invention would need to solve an entirely different set of problems than those solved by Serret-Avila. Whereas Serret-Avila solves problems pertaining to very large media files, the present invention involves managing only a small amount of data, namely, rights and usage information. Whereas Serret-Avila pertains to "smart" client devices that are capable of receiving streamed data, as across a network or of otherwise receiving very large blocks of data, *see, e.g.* Serret-Avila, column 3, lines 17-19, 27-30, 47-53, 59-66, the present invention involves a client that may not even be capable of external communication, *see* Current Application paragraph [0006]. Whereas Serret-Avila describes as unsatisfactory approaches to authentication that rely on a client's having the entirety of a set of data, *see* Serret-Avila, column 2, lines 8-33, the present invention pertains largely to clients that have a complete set of usage and rights information.

The last point is worth repeating because it indicates that Serret-Avila teaches away from the solutions described in the present invention. The present invention most typically pertains to a client device that stores a set of rights and/or usage information, *see* Current Application, paragraph [0017], a set of information that must be kept safe from tampering, but a set of information that is most desirably kept in clear form. The problem solved by the present invention, then, is how a client device may simply maintain the integrity of a relatively small set of data, data that is most conveniently stored in clear form. Serret-Avila explicitly rejects as problematic approaches that rely for authentication on a client's possessing an entire set of data. In short, contrary to the Examiner's suggestion, a person of ordinary skill working with the subject matter of the present invention would have had no need to enable fast, secure, and efficient authentication of data streams, as taught by Serret-Avila. Accordingly, Claims 5, 7, 25, 40, 53, 55 are allowable.

Claims 10, 32, 33, 43, 58

In the Office Action, Claims 10, 32, 33, 43, 58 were rejected as being obvious considering Nonaka in view of Chase's US Patent No. 7,080,043 (hereinafter "Chase"). Applicant respectfully submits that these claims are patentable over Nonaka in view of Chase.

As an initial matter, Claims 10, 32, 33, 43, 58 all depend from independent Claims that are allowable because, as discussed above, Nonaka does not teach or suggest storing rights information in clear form. Therefore, Claims 10, 32, 33, 43, 58 are allowable because they

depend from allowable independent claims. However, Claims 10, 32, 33, 43, 58 are also allowable for additional reasons. The following is a nonexclusive listing of additional reasons why Claims 10, 32, 33, 43, 58 are allowable.

Even considering Nonaka in view of Chase, disabling content on the client device would not have been obvious to a person of ordinary skill in the art because Chase relies on interaction with an external license server to manage content revocation. *See* Chase, column 34, lines 23-24. Chase teaches that client devices must communicate with a license server that will make determinations about issuing and/or revoking rights information. *See id.* Furthermore, Chase teaches that a content owner "wants the ability to disable access to its content across all applications without having to identify each application or component." Chase, column 33, lines 54-56. By contrast, in the present invention, each client device makes the individual determination as to whether to disable content one at a time. No license server is needed. Indeed, clients using the present invention need not have the capability of external communication. *See* Current Application, paragraph [0006]. Accordingly, one of ordinary skill in the art would not have been motivated to consider Nonaka in view of Chase. Therefore, Claims 10, 32, 33, 43, 58 are allowable.

CONCLUSION

Applicant submits that all pending claims are in condition for allowance. Accordingly, early and favorable action allowing all of the pending claims and passing this application to issue is respectfully requested. The Examiner is invited to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

Applicants believe that no fees are required. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to our firm's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW GROUP

Date: April 9, 2007

by: /Adam L.K. Philipp/
Adam L.K. Philipp
Reg. No.: 42,071

AXIOS LAW GROUP
1725 Westlake Avenue N
Suite 150
Seattle, WA 98109
Telephone: 206-217-2200